

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: PROXIMITY BASED SECURITY PROTOCOL
FOR PROCESSOR-BASED SYSTEMS

INVENTOR: Jeffrey L. Huckins

Express Mail No. EV 337 932 365 US

Date: July 31, 2003

PROXIMITY BASED SECURITY PROTOCOL
FOR PROCESSOR-BASED SYSTEMS

Background

This invention relates generally to processor-based systems.

Processor-based systems may be wired or wireless,
5 portable and less portable. Wired devices may be connected
by physical wires to one another and to electrical
connections. A portable device may be coupled by wireless
signals to other devices and may use a battery as a source
of power. Portable processor-based systems include, for
10 example, laptop computers, cellular telephones, handheld
devices, and personal digital assistants.

Processor-based systems are subject to two security
concerns. The first concern relates to the security of the
data actually stored on the processor-based system. The
15 second security concern relates to the potential theft of
the processor-based system. Particularly with portable
processor-based systems, theft is easy.

Thus, there is a need for better ways to provide
security for processor-based systems.

20 Brief Description of the Drawings

Figure 1 is a schematic depiction of one embodiment of
the present invention;

Figure 2 is a flow chart of a first embodiment of software for securing a processor-based system;

Figure 3 is a flow chart for a second embodiment for securing a processor-based system;

5 Figure 4 is a flow chart for a remote or handheld device in accordance with one embodiment of the present invention;

Figure 5 is a schematic depiction of a processor-based system to be secured in accordance with one embodiment of
10 the present invention; and

Figure 6 is a schematic depiction of a remote or handheld device in accordance with one embodiment of the present invention.

Detailed Description

15 Referring to Figure 1, a processor-based device 12 may be associated with a handheld or portable device 14. The processor-based system 12 may be a portable, battery powered device in accordance with one embodiment of the present invention. It may also be capable of wireless
20 communication over one or more wireless protocols. For example, the processor-based system 12 may communicate over a first wireless protocol 15 with a device 14 in the form of a cellular telephone and over a second wireless protocol 13 with an access point 16.

25 The wireless protocol 15 may be a short range wireless protocol having a range, for example, on the order of about

ten feet. One such protocol having such a range is described as the Bluetooth Specification V.1.0B (2003). The range of the protocol 15 is indicated by the arrow A. So long as the handheld device 14 is within the distance A of the processor-based system 12, wireless communication is possible. If the device 14 strays into the region B, wireless communication may no longer be established.

Thus, a network 10 may be formed of the devices 12, 14, and 16, as well as other devices. The range of the wireless network 10 may be limited by the range of the various wireless protocols 13 and 15 that may be utilized.

The processor-based device 12 may be a laptop computer in one embodiment of the present invention. Laptop computers are particularly prone to being stolen. However, the processor-based device 12 may be any processor-based device.

In one embodiment of the present invention, the user may carry the handheld device 14 on his or her person, for example in the user's pocket or it may be held in the user's hand. Thus, the handheld device 14 is closely associated with the location of a user. That same user may own a processor-based system 12. When the user strays beyond the distance A, wireless communication with the processor-based system 12 is discontinued. This may be used as an indication that someone who is attempting to use the processor-based system 12 is unauthorized. Since it

can be determined that the authorized user is not proximate to the processor-based system 12, the system 12 may determine that it is not appropriate to allow the person attempting to use the processor-based system to have
5 access. This may provide data security, preventing the unauthorized user from accessing the computer. It may also provide physical security since there is no incentive to steal the processor-based system 12 if it can never be used.

10 Thus, in one embodiment of the present invention, the system 12 determines whether the user is proximate by attempting to establish wireless communications with the handheld device 14. If such communications are not possible, the processor-based system 12 implements a
15 security protocol that may include denying access, initiating a phone call to the user or others, initiating an alarm, or simply turning the processor-based system 12 permanently off.

Referring the Figure 2, in accordance with one
20 embodiment of the present invention, the access control software 20a may be resident on the processor-based system 12. Initially, it determines whether there is a request for access as indicated at diamond 22. If so, a proximity check is implemented as determined in diamond 24. In one
25 embodiment, the proximity check may simply determine whether communication is possible with the handheld device

14. In one embodiment of the present invention, various wireless protocols, such as the Bluetooth protocol, may automatically provide an indication of sufficiently proximate devices and their identifiers. If no such communication can be established with the handheld device 14 normally carried by the user's person, a secure system command 28 may be issued. The secure system command 28 may prevent access, may activate an alarm, may automatically initiate a telephone call to an appropriate entity to provide security, or any of a variety of other actions. If the proximity check is successful, access may be allowed as indicated in block 26.

In accordance with another embodiment of the present invention, shown in Figure 3, the access control software may also initially receive a request for access as indicated in diamond 22. Upon receiving a request for access, the handheld device 14 may be automatically contacted as indicated in block 32. Only if the authorization code is received from the handheld device 14, as determined in diamond 34, is access allowed, as indicated in block 26. Otherwise the system 12 is secured as indicated in block 28. In some cases, requiring the access protocol may be a more reliable way of ensuring that access is not permitted when the user is not proximate to the access processor-based system 12.

In accordance with one embodiment of the present invention, the handheld device 14 may include the software 22 shown in Figure 4. When a mobile access contact is implemented, as indicated at block 30, an authentication
5 protocol is implemented. If the access contact is the remote processor-based system 12, security credentials may be provided as indicated in block 32. Of course, if the handheld device 14 is outside the wireless range of the processor-based system 12, the security credentials will
10 never be received and, therefore, access will not be permitted.

In another embodiment, a distance measurement solution may be used. For example, a signal strength indication (SSI) may be used to determine whether the user is farther
15 from the system 12 than a predetermined distance.

Referring to Figure 5, one exemplary architecture for the processor-based system 12 is illustrated. Of course, any other architecture may be utilized as well. In the illustrated architecture, the processor 40 is coupled by a
20 bus 42 to an input/output device 46. A wireless interface 44 may implement one or more appropriate wireless protocols, including a short range wireless protocol, such as the Bluetooth protocol. The wireless interface may be coupled to an antenna 50 such as a dipole antenna.

25 The bus 42 may also be coupled to a storage device 45 and in one embodiment of the present invention may be a

hard disk drive and in another embodiment of the present invention may be a semiconductor memory. The storage 45 may store the access control software 20a and 20b.

Referring to Figure 6, the handheld device 14 may have the exemplary architecture illustrated. As mentioned above, the architecture illustrated is only one example of a potential architecture for implementing the handheld device 14. In this embodiment, a processor 40 is coupled through a bus 42 to the wireless interface 44 and the input/output device 46. The antenna 50 is coupled to the interface 44. The storage device 45 may store the software 20c in one embodiment of the present invention. The storage device 45 may be a semiconductor memory such as a flash memory. However, it can also be any other type of non-volatile storage including a hard disk drive.

Any suitable authentication protocol on the processor-based device 12 and the handheld device 14 may be utilized for exchanging credentials. As an example, an 802.1X supplicant on a handheld device 14 and an 802.1X authenticator on the processor-based system 12 may be used to exchange credentials using the Bluetooth personal area network (PAN) profile. For example, the 802.1X protocol may be the IEEE 802.11 protocols currently specified or their successors. See IEEE 802.11 (1999) specification available from IEEE, New York, New York (ISBN 0-7381-2315-3; Product No.: SH94842-TBR). Security credentials may be

stored on the handheld device 14 and a subscriber information module (SIM) 52 to perform the 802.1X authentication of user and processor-based system 12 to the network 10. In this way, a single SIM 52 in the user's
5 handheld device 14 serves multiple functions, including user authentication to the handheld device by a personal identification number protected access, user and handheld device authentication to the processor-based system 12, user and processor-based system 12 authentication to a
10 network 10, for example via 802.1X, and verification of user possession of the processor-based system 12. An 802.1X supplicant on the processor-based system 12 may then use these credentials to respond to an 802.1X authentication protocol from an 802.11 access point 16.

15 While the present invention has been described with respect to a limited number of embodiments, those skilled in the art will appreciate numerous modifications and variations therefrom. It is intended that the appended claims cover all such modifications and variations as fall
20 within the true spirit and scope of this present invention.

What is claimed is: